WEST

Help   Logout

Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents
First Hit | Previous Document | Next Document
Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC

Document Number 4

Entry 4 of 52   File: USPT   Nov 23, 1999

DOCUMENT-IDENTIFIER: US 5991735 A
TITLE: Computer program apparatus for determining behavioral profile of
a computer user

BSPR:
One of the largest pools of databases and electronic media is found on
The Internet. The World Wide Web (Web) is a two-year-old protocol used
to create and publish documents on the Internet. Web documents may
contain graphics, text, sound, video or any combination of these. Web
documents can include "hyperlinks" which are highlighted areas of
information in one document that, when user-selected, open a related
document. In late 1994, "forms" were added to the Web to make it
interactive. Previously, Web pages could only be used to display
information or point to other Web sites where information was available.
The 1994 change allowed those publishing Web pages to publish "forms",
i.e., documents that include blank spaces to be completed by users and
then returned to the publishing computer, thus allowing interactivity.

BSPR:
Other examples of businesses that offer agate information on the
Internet are Movie Phone whose World Wide Web Site is WWW.777film.com
and Securities APL (at WWW.secapl.com) which allows users to look up
individual stock quotes (delayed 15 minutes).

DEPR:
In particular, in response to user login, program controller 79 checks
with the user profiling member 73 to determine whether the user has in
the past logged on to program 31 or is a new user. In the former case,
according to records in the user profiling member 73, the program
controller 79 obtains preference information for that user and using
agate information from the agate data assembly 71 generates an initial
screen view formatted according to the user's recorded preferences.
Program controller 79 transmits the generated screen view through Web
server 27 for display to the user.

DEPR:
In the latter case (a first time/new user), program controller 79
assigns a unique users computer ID upon user login. This, in turn,
enables user profiling member 73 to initialize tracking of viewing
activity of the new user immediately following login. Program controller
79 obtains initial agate information from agate data assembly 71 to
display the Home Page to the new user. Program controller 79 also
obtains user identification information from the user to assign a user
name and password at the user's convenience.

DEPR:
Stored locally on a user's PC is a cookie (technology by Digital
Equipment Corp.) for identifying the user and his preferences. The user
logs onto the Internet 29 and enters the URL or Website address of
program 31 which initializes main routine 39. The URL request is
received by Web server 27 which in turn transmits (a) a login
advertisement screen view (i.e., from Page Oobjects 35a,b,c and Ad

Package Object 33b) and (b) a request for a cookie that indicates whether this is a first time user. When no cookie is present, the main routine 39 transmits through server 27 the standard introductory screen view page (Home Page 43, FIG. 4a).

DEPR:
Preferably the Home Page 43 (FIG. 4a) is an HTML (HyperText) document generated through the set of Page Objects 35a,b,c. The Home Page 43 describes to new users the data available at the program 31 Website and allows existing users to log in. The Home Page 43 is formed of several graphical and text documents in the HTML and Java formats. For example, behind the "stock data" menu selection a Stock Exchange ticker flashes, and behind the "weather" option, a display of clouds swirling over San Francisco and then sunshine over Washington, D.C. is shown. A clip of a newly released movie plays behind the "Media Schedule" option, and sports scores scroll behind the "Sports" option. At the bottom of the screen view are login fields and prompts.

DEPR:
For a new user, the Home Page 43 effectively requests a user name and password. In response to the user-provided data, main routine 39 immediately builds a cookie if possible. Included in the newly built cookie is a unique user identification code (preferably numeric), time and date of login, and computer identification number to distinguish between home and work logins. Main routine 39/server 27 transmits the created cookie to the user's PC for storage and future use.

DEPR:
Program 31 a--so creates a new User Object 37a, User Computer Object 37b, User Interface Object 37c, User Session Object 37d, User Action History Object 37e and User Viewing History Object 37f for the new user. User Object 37a records the user-provided name and password used to create the cookie. User Session Object 37d records the login time. User Action History Object 37e records the selection activity of the user. The User Viewing History Object 37f also registers the open and leave times for the initial login advertisement screen view and notes what elements were displayed at that time. Also the Ad Package Object 33b responsible for the initial login advertisement screen view records a "hit" by the new user.

DEPR:
In response to the user's selection and entered stock symbol, a long URL is generated and received by server 27. While no page currently exists at the requested address (the URL), program 31 generates one in response. Specifically, main routine 39 queries the Financial Page Object 35a,b,c (Appendix I) and requests the standard "quick quotation". The Page Objects 35a,b,c assemble the data, format it into a table and return it to Web server 27. Sources of the data include on-line securities information from S & P Comstock and information stored by age Data Objects 35b.

DEPR:
Subsequently when the sponsor-user logs on, the Web server 27 (using cookies if available) identifies the sponsor-user with a user ID stored in the Sponsor Object 33a (FIG. 5a). Preferably, separate cookies are used to identify the user's personal login apart from that of the user as an agent of a sponsor-company. Also program 31 begins recording page information for the sponsor, and begins building a demographic and psychographic profile and usage history upon the sponsor-user entering the system.

DEPR:
Subsequent login to program 31 completes a similar query to the one above, this time checking for both of the sponsor's advertisements. Reporting subroutine 41 generates a report: listing the successes of the ads in two columns of a table. To accomplish this, subroutine 41 uses Sponsor Object 33a, Ad Package, Ad Series and Ad Objects 33b, 33c and 33d.
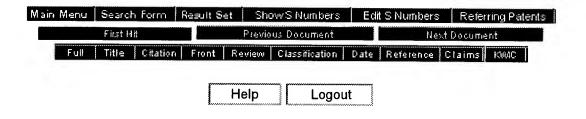
DEPR:
Program 31 typically gives users a quick glimpse at the 5-day forecast
on the login page, with additional information about their local area or
others in map format, graphical images (e.g., a snowflake), and data.
Weather summaries may be available (short text blurbs) for larger
regions, and possibly for individual cities.

ORPL:
"Ipro," http://www.ipro.com/, Internet profiles Corporation Home and
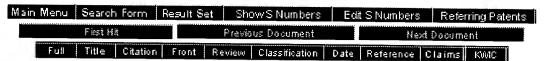other Web Pages (Jul. 11, 1996).

ORPL:
Betts, M., "Sentry cuts access to naughty bits," Computers and Security,
vol. 14, No. 7, p. 615 (1995).

Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents

First Hit	Previous Document	Next Document

Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Help	Logout

WEST

Help	Logout

Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents

First Hit	Previous Document	Next Document

Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Document Number 10

Entry 10 of 52   File: USPT   Oct 19, 1999

US-PAT-NO: 5970499
DOCUMENT-IDENTIFIER: US 5970499 A
TITLE: Method and apparatus for producing and accessing composite data
DATE-ISSUED: October 19, 1999
US-CL-CURRENT: 707/104; 707/102
APPL-NO: 8/ 832688
DATE FILED: April 11, 1997

WEST

Document Number 10

Entry 10 of 52   File: USPT   Oct 19, 1999

DOCUMENT-IDENTIFIER: US 5970499 A
TITLE: Method and apparatus for producing and accessing composite data

DEPR:
The client computer then generates request 246 for composite data 244
(step 304). Request 246 includes, for example, an operator identifier,
security screening information, and treatment information. The client
computer also transmits or enables transmission of (from a radiological
database, for example) collected patient data 200 and associated
filtering context 242 to the server computer (step 306).

DEPR:
FIG. 7 is a block diagram of a facility consistent with the present
invention for providing composite data across a computer network to
customers under a service contract. In FIG. 7, solid lines indicate a
path for both control and data flow and dotted lines indicate data flow
only. Facility 700 is preferably connected to a wide area network, such
as Internet 701, through firewall 702. Firewall 702 is a computer that
monitors all data traffic into and out of facility 700 to prevent
unauthorized access to the facility. World Wide Web page 704 provides a
graphical user interface to access facility 700. Facility 700 also
includes customer account manager 710, which controls functions
available to customers with service contracts authorizing access to
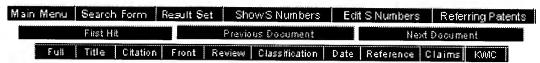facility 700.

DEPR:
User login authentication is performed by customer account manager 710
and control is passed to one of three processes, service request manager
706, customer database manager 708, or results manager 712 depending on
the service that the customer chooses. Customers that wish to initiate a
new request for composite data are passed to service request manager
706. After successful completion of a composite data request, the
customer's account is billed and the status of any pending requests is
provided. Customers that wish to view the composite data generated in
response to the request are passed to results manager 712. Information
pertaining to a customer's account (e.g., billing information, changing
passwords, user preferences, etc.) may be obtained by submitting queries
to customer database manager 708.

WEST

Help   Logout

Main Menu | Search Form | Result Set | Show S Numbers | Edit S Numbers | Referring Patents
First Hit | Previous Document | Next Document
Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC

Document Number 31

Entry 31 of 52   File: USPT   Apr 27, 1999

US-PAT-NO: 5898780
DOCUMENT-IDENTIFIER: US 5898780 A
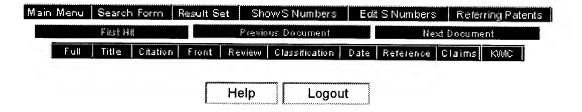TITLE: Method and apparatus for authorizing remote internet access
DATE-ISSUED: April 27, 1999
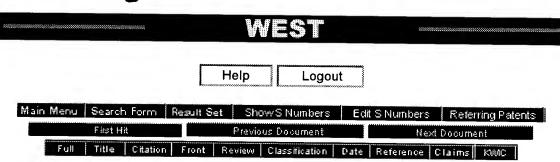US-CL-CURRENT: 713/155; 705/18
APPL-NO: 8/ 727996
DATE FILED: October 9, 1996
PARENT-CASE:
This application claims priority of provisional patent application
60/017,682, filed May 21, 1996.

WEST

| Help | Logout |

Main Menu	Search Form	Result Set	Show S Numbers	Edit S Numbers	Referring Patents
First Hit	Previous Document	Next Document
Full	Title	Citation	Front	Review	Classification	Date	Reference	Claims	KWIC

Document Number 31

Entry 31 of 52   File: USPT   Apr 27, 1999

DOCUMENT-IDENTIFIER: US 5898780 A
TITLE: Method and apparatus for authorizing remote internet access

ABPL:
A method and apparatus for allowing a user to access the internet from a
remote location by using a local internet service provider with whom the
user does not have an account. The user logs on to the local internet
service provider's system using an identifier that includes the user's
identification term and an identifier for the user's home internet
service provider server. A first server in the local internet service
provider's system determines that the login information includes the
identifier for the user's home internet service provider server and
sends a query to a second server. The second server verifies that the
user's home internet service provider has an account with the local
internet service provider and returns an internet protocol address for
the home internet service provider's server to the first server. The
first server then seeks authorization from the home internet service
provider's server to provide internet access to the user over the local
internet service provider's system.

BSPR:
The present invention comprises a method and apparatus for allowing a
user to access the internet from a remote location by using the local
network of a local internet service provider. For purposes of this
patent application, a local (also called foreign) internet service
provider is an internet service provider with whom the user does not
have an account. The internet service provider (ISP) with whom the user
does have an account is referred to as the home internet service
provider (home ISP). The apparatus of the present invention comprises a
server or servers that can recognize the domain name of the home ISP in
the login information provided by the user. The server or servers can
also verify that the domain name of the home ISP is listed with the
local ISP and can retreive an internet protocol (IP) address and related
information for the server having the domain name of the home ISP.

BSPR:
In an embodiment of the present invention referred to as a peer-to-peer
system, a specially modified authentication server in the local internet
service provider's system detects that the login information includes
the identification term for the server of the home ISP. The server then
verifies that the user's home internet service provider has an account
with the local internet service provider and then seeks authorization
from the home internet service provider server to provide internet
access to the user.

DEPR:
FIG. 4 illustrates the functions performed by the user recognition
module 54. In block 80, a user has used the remote computer 26 to
connect to the modem rack 18 of a local internet service provider. In
the method of the present invention a user who is not a customer of the
local internet service provider logs in using the following format: a
user identifier plus a home ISP identifier plus a password. For example,

an acceptable login format might be of the form username@userdomain,
where the term userdomain is the domain name of the user's home internet
service provider, and the term user name is the user identification used
with the user's home internet service provider. For example, the login
could be jdoe@aimnet.com, which is a typical e-mail address. Normally a
password will also be used in the login process.

DEPR:
In block 84, the user recognition module 54 looks to see if the home ISP
identifier, for example the term @userdomain, is in the login field. If
it is, then in block 88, the home ISP identifier is checked against the
host table 58 (shown in FIG. 2) to verify that the home ISP identifier
(i.e. the user's home internet service provider) is registered with the
local internet service provider. Block 92 illustrates that access to the
internet is denied if the home ISP identifier is not listed in the host
table 58. If the home ISP identifier is listed in the host table 58, the
server 14 routes the username (and password) to the home internet
service provider system 64 via the router 34, the internet link 65 and
the router 66. In block 96, the user authentication server 68 then
verifies that the user is a customer of the home internet service
provider (e.g. has an account and is in good standing). If the server 68
decides that the user is a customer of the home internet service
provider, then in block 100, the server 68 sends an authorization
message back to the local internet service provider system 63, via the
internet connection 65. Alternatively, the server 68 can deny
authorization as indicated at block 104.

DEPR:
Comparing FIG. 5 to FIG. 3 illustrates that the system 120 includes the
routing servers 136 and 138 which are not present in the system shown in
FIG. 3. FIG. 6 illustrates the way the server 136 functions in the
system 120. The user 144 connects to the system 120 via the dialer 124
and transmits login information as was described previously with respect
to FIG. 4. At block 150, the network server 128 issues a request to
authenticate the login information. At block 154, the server 132
determines whether or not the login information contains a "roaming"
designation such as the @ character followed by additional user
information. If roaming information is detected, the server 132 queries
the login information to the routing server 136 as indicated by block
158.

DEPR:
Block 162 indicates that the server 136 includes software that attempts
to match the "roaming" login information with an entry in a log table in
the server 136. If the server 136 can make a match, then at block 166
the server 136 returns information to the server 132 that includes an IP
address for a server that has the domain name contained in the login
information provided by the user 144. The server 132 then sends an
authentication request containing the user's name and password to the
server 140. The server 140 checks this information and at block 170,
transmits a message to the server 132 either stating that the user 144
should be granted or denied internet access.

DEPR:
Block 174 indicates that if the server 136 cannot match the "roaming"
login information, then a message is sent to the server 132 stating that
internet access should be denied to the user 144.

DEPR:
In another situation, if no roaming information was detected at block
154, then at block 176, the server 132 processes the login information
to determine if the user is a customer of the local ISP. The decision to
accept or reject the user is then based solely on the user
authentication information maintained by the local ISP.

DEPR:
FIG. 7 illustrates the general flow of the searching function performed
by the routing server 136. Beginning with block 158 (also shown in FIG.
6), a query is sent to the server 136 by the server 132. Typically, if

the login information for the user 144 is in the form of username@userdomain plus password, the username and password are stripped away so that the query only asks the server 136 if it can verify the userdomain information and provide an internet address for the server identified by the userdomain term. The server 136 checks its authentication table. At block 184, if the server 136 finds a match with the userdomain transmitted in the query, the server 136 returns an internet protocol (IP) address for the userdomain to the server 132, along with other information such as the port number, authentication type and time zone difference. In the preferred embodiment, RADIUS type authentication is used. But other authentication types, such as TACACS+ could be used.

DEPR:
Referring to FIGS. 5-9, the overall flow of information in the system 120 can now be discussed. The user 144 uses the dialer 124 to connect to a local internet service provider (local ISP) and transmits a user identifier plus a home ISP identifier plus a password to the server 132. For example, an acceptable logon format might be of the form username@userdomain plus a password. Typically, the password will be in a UNIX password file or in a third party's security server, such as Kerberos. Also, the password is typically encrypted (MD5) when sent from the server 132 to the server 140. An encryption key is shared between the servers 132, 136 and 140.

DEPR:
Referring to the server 132, the function of this server is to receive authentication requests from the server 128. If the authentication request comes from a regular customer login (i.e. a customer who has an account with the local ISP), then normal user id and password authentication is performed as is well-known in the prior art. If the user requesting authentication is a "roamer" (i.e. a customer who does not have an account with the local ISP), the roamer transmits identifying information to the server 128 in the form of username@userdomain plus a password. The server 132 detects that this is a roamer because of the @ character, and sends a query to the closest routing server 136. The server 136 processes the query, as explained previously with respect to FIGS. 6-8, and sends the results of its search back to the server 132. If the results include identification of a home ISP server (i.e. the server 140), then the server 132 transmits an authentication request to the server 140 for verification of the user id (username) and password.

DEPR:
The server 132 also receives accounting data from the server 128. If the data is for a regular customer login, the data is written to the Local ISP log file on the server 132. If the data is for a roamer, the data is written to the Home ISP log file on the server 132 and on a log file in the server 136 and in the server 140.

CLPR:
5. The method of claim 4 wherein the server identification information is separated from the user identification information by the @ symbol in the login information packet.

CLPR:
12. The method of claim 11 wherein the server identification information is separated from the user identification information by the @ symbol in the login information packet.

CLPV:
receiving a login information packet at a first server from a user, the login information packet including user identification information that is used to identify the user and home server identification information that is used to determine an internet address for a second server that uses the user identification information to identify the user;

CLPV:
determining that the login information packet includes the home server

identification information;

CLPV:
receiving a <u>login</u> information packet at a first server from a user, the
<u>login</u> information packet including user identification information that
is used to identify the user and server identification information that
is used to determine an internet address for a second server that uses
the user identification information to identify the user;

CLPV:
receiving a <u>login</u> information packet at a first server from a user, the
<u>login</u> information packet including user identification information that
is used to identify the user and server identification information that
is used to determine an internet address for a second server that uses
the user identification information to identify the user;

CLPV:
a first server for receiving a <u>login</u> information packet from a user, the
<u>login</u> information packet including user identification information that
is used to identify the user and server identification information that
is used to determine an internet address for a second server that uses
the user identification information to identify the user;

ORPL:
iPass Inc.-True Global Internet Roaming, <u>web page,</u> http://www.ipass.com
(Sep. 14, 1998) p. 1.

ORPL:
iPass Services-Service Overview (Whitepaper), <u>web page,</u>
http//www.ipass.com/services/isp-whitepaper.html (Oct. 28, 1998) pp.
1-12.

ORPL:
iPass Services-Become a Global Provider Today, <u>web page,</u>
http://www.ipass.com/services/isp.html (Oct. 28, 1998) pp. 1-3.

ORPL:
iPass Inc.--True Global Internet Roaming, <u>web page,</u>
http://www.ipass.com/ (1997).

WEST

| Help | Logout |

| Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers |

| Generate Collection |

Search Results - Record(s) 1 through 2 of 2 returned.

☐ 1. Document ID: US 5991735 A

Entry 1 of 2   File: USPT   Nov 23, 1999

```
US-PAT-NO: 5991735
DOCUMENT-IDENTIFIER: US 5991735 A
TITLE: Computer program apparatus for determining behavioral profile of a computer
user
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Image |

☐ 2. Document ID: US 5848396 A

Entry 2 of 2   File: USPT   Dec 8, 1998

```
US-PAT-NO: 5848396
DOCUMENT-IDENTIFIER: US 5848396 A
TITLE: Method and apparatus for determining behavioral profile of a computer user
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Image |

| Generate Collection |

Terms	Documents
l10 and identify	2

| Display 10 Documents | including document number | 2 |

Display Format: TI | Change Format |

| Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers |

| Help | Logout |